wavecom

Connecting every...things

Creative and innovative solutions in the field of communications engineering.

Coordinated Vulnerability Disclosure Policy

September 2026

Table of Contents

1. Document Control

> *EU 2024/2847 (CRA)- Art. 13(8): Manufacturers must have policies and procedures in place to handle vulnerabilities. A policy document must exist, be versioned, owned, and reviewed regularly.*

Field	Wavecom
Organisation Name	WAVECOM – Soluções Rádio, S.A.
Document Owner	Information Security Manager (ISM)
Security Team Name	Wavecom Product Security Incident Response Team (PSIRT) — under constitution. Until it is formally established, the function is performed by the Information Security Manager together with the R&D Department.
Version	1.0
Effective Date	8th September 2026
Review Cycle	Annual, or earlier following a significant product change or a change in the applicable CRA framework
Classification	Public

2. Purpose Statement

WAVECOM is committed to the security of the products with digital elements it places on the market. This **Coordinated Vulnerability Disclosure (CVD) Policy** describes how external parties — including security researchers, customers, and members of the public — may report potential security vulnerabilities in our products and systems, and how we will handle those reports.

This policy is aligned with Regulation (EU) 2024/2847 (the Cyber Resilience Act — CRA) and prEN 40000-1-3 which establishes requirements and recommendations for manufacturers of products with digital elements on disclosure of potential vulnerabilities in products.

3. Roles and Responsibilities

> *EU 2024/2847 CRA- Art. 13(17): Manufacturers must designate a single point of contact. The contact must be easily identifiable, allow users to choose their preferred means of communication, and must not be limited to automated tools.*

3.1 Internal Security Team

The designated internal team responsible for managing vulnerability disclosure is the Wavecom Product Security Incident Response Team (PSIRT). This team is responsible for:

Receive and acknowledge reported vulnerabilities.

Validate, assess, and prioritise vulnerabilities based on risk.

Coordinate remediation activities with relevant internal teams.

Manage communication activities throughout the vulnerability handling process.

Issue vulnerability advisories and notifications, where appropriate.

Field	Wavecom
Team or person responsible for receiving reports	Information Security Manager (ISM), acting as the CRA single point of contact and monitoring ciberseguranca@wavecom.pt.
Does a formal PSIRT exist?	Cybersecurity activities are currently shared across the Wavecom technical team. A dedicated PSIRT is planned for the future.
Who coordinates remediation?	R&D Department, together with the Product Security Owner for the affected product line.
Who approves public disclosure?	Board of Directors, on a proposal from the ISM.

3.2 What We Ask of Vulnerability Reporters

Any individual or organisation that submits a vulnerability report is expected to act in good faith and comply with the following:

- Do not attempt to exploit the vulnerability beyond what is needed to confirm its existence.
- Do not access, modify, or exfiltrate data beyond what is strictly necessary to demonstrate the issue.
- Do not disclose the vulnerability publicly before we have had a reasonable

opportunity to investigate and fix it.

- Provide enough information for us to reproduce, assess, and validate the reported issue.
- Do not conduct denial-of-service attacks, social engineering, or phishing as part of any testing.

4. Scope of This Policy

> *CRA / prEN 40000-1-3: [PRE-2-RC-02]: The vulnerability disclosure policy should specify the secure communication options, scope, publication, recognition and vulnerability reporting contents. EU 2024/2847 CRA- Annex I Part I, point (2)(a): Products must be placed on the market without known exploitable vulnerabilities — which requires a process to receive reports about them.*

4.1 Products and Systems Covered by This Policy

The following systems, products and services are within the scope of this policy:

Product / System Name	Version/ URL/ Scope Details	Includes Cloud / App?
Wavecom IoT Gateway	WR, WK and WT ranges — all supported hardware revisions and firmware versions placed on the EU market, including units placed before 11 September 2026 (CRA Art. 69(3)) Operating system running on Wavecom IoT Gateway WR series hardware – WaveOS – 2025+ releases.	Yes — managed through Wavecom IoT Manager
Wavecom IoT Manager	Centralized WEB platform in SaaS and on-premises deployments — all supported versions containing: Gateway management and provisioning service; Device management and provision service; Fleet monitoring service; Water monitoring service.	No

Product / System Name	Version/ URL/ Scope Details	Includes Cloud / App?
Cloud Authentication System (CAS)	Wi-Fi guest authentication and access control service, in SaaS and on-premises deployments, integrated on Wavecom IoT Manager platform or standalone.	No
WHERE IS®	RTLS and RFID location platform, including the Wavecom developed software components, in SaaS and on-premises deployments; third-party hardware is covered by its own manufacturers.	No

4.2 What Is Not Covered (Out of Scope)

The following are outside the scope of this policy. Reports relating to these will not be investigated:

- Third-party products, services, or infrastructure not owned or operated by Wavecom.
- Social engineering, phishing, or physical security attacks against Wavecom or its staff.
- Denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks.
- Products or software versions that have reached end of life and are no longer supported.
- Vulnerabilities already known to Wavecom or already reported by another party.

5. How to Report a Vulnerability

> *EU 2024/2847 CRA- Art. 13(17): The single point of contact must be easily identifiable, allow the user to choose their preferred means of communication, and must not be limited to automated tools. prEN 40000-1-3: [PRE-2-RQ-02]- One or more contact mechanisms must exist. [RCP-1-RQ-01]: The contact mechanisms must be accessible to the public.*

5.1 Contact Channels

Channel	Required?	Details
Security email address	Required — must be a monitored inbox	ciberseguranca@wavecom.pt — monitored inbox, operated by the Information Security Manager (ISM) as the CRA single point of contact under Art. 13(17). Acknowledgement within 3-5 business days.
Phone / customer service	Optional — useful if you have an existing support line	Wavecom Technical Support may receive reports through the usual customer support channels. Support and field engineering teams are instructed to forward any indication of a security vulnerability or of active exploitation immediately to ciberseguranca@wavecom.pt, and by telephone where exploitation is suspected, without prior technical assessment.
PGP key (for encrypted email)	Recommended if email is your primary channel — allows reporters to send sensitive information securely	Not currently published. Reporters who need to transmit sensitive information should request encryption arrangements at ciberseguranca@wavecom.pt.

5.2 What Reporters Should Include in Their Report

> *CRA / prEN 40000-1-3: [PRE-2-RC-02]: The vulnerability disclosure policy should specify the content of expected vulnerability reports.*

We ask reporters to include, as a minimum, the following information where possible. This helps us triage and investigate reports quickly:

- The affected product name, model, version, and/or URL.
- A clear description of the vulnerability and its potential security impact.
- Step-by-step instructions to reproduce the vulnerability, including any tools or configurations used.
- Supporting evidence — screenshots, network captures, log files, or proof-of-concept code.
- A suggested severity rating or CVSS score if available (this is optional).

- Contact details for follow-up communication — anonymous reports are also accepted.

6. Vulnerability Handling

> *CRA / prEN 40000-1-3: [PRE-2-RQ-03]: The expectations for communication with the reporter must be described. EU 2024/2847 CRA- Annex I Part II, point (2): Vulnerabilities must be addressed and remediated without undue delay including by providing security updates.*

6.1 Acknowledgement

> *CRA / prEN 40000-1-3: [RCP-1-RQ-02]: Every report must be assigned a tracking number. [RCP-1-RQ-03]: Acknowledgement must be sent within the timeframe stated in this policy.*

Upon receipt of a potential vulnerability report, Wavecom will acknowledge receipt within the period stated below. The acknowledgement will include a unique tracking number.

WAVECOM acknowledges all vulnerability reports within 3-5 business days of receipt. The acknowledgement includes a unique tracking number, which the reporter should quote in any subsequent correspondence.

6.2 Triage and Verification

> *CRA / prEN 40000-1-3: [VRF-1-RQ-01]: If the initial report does not contain sufficient information to reproduce the vulnerability, the reporter must be contacted to request additional details.*

Following acknowledgement, the security team will assess the report within the defined timeframe. During this assessment, Wavecom will:

- Validate and reproduce the reported vulnerabilities.
- Assess severity using an established scoring system (CVSS v3.1).
- Identify affected products/versions.
- Assign priority and responsible remediation owner.

If the submitted report does not contain sufficient information to reproduce the

vulnerability, the security team will contact the reporter to request the required additional details.

WAVECOM completes initial triage and provides a status update to the reporter within 7 business days of acknowledgement. Where the report concerns a vulnerability that is being actively exploited, triage begins immediately and the CRA Article 14 reporting process is activated in parallel, independently of the communication with the reporter.

6.3 Remediation Timelines

> *prEN 40000-1-3: [RMD-2-RQ-01]: Remediation must be developed and [RMD-3-RQ-01]: Remediation must be tested.*

WAVECOM aims to fix validated vulnerabilities within the following target timelines, based on severity:

Severity	Target Timeline
Critical / High (CVSS ≥ 7.0)	30 calendar days
Medium (CVSS 4.0 – 6.9)	60 calendar days
Low (CVSS < 4.0)	90 calendar days
Special cases (if applicable)	Field equipment that can only be updated during a scheduled maintenance window, and vulnerabilities in third-party components awaiting a supplier fix. Extended timelines are agreed with the reporter in advance, justified in writing and recorded.

Severity and Response Time Scale

LOW	MEDIUM	HIGH	CRITICAL
CVSS 0.1–3.9 Target fix: 90 days	CVSS 4.0–6.9 Target fix: 60 days	CVSS 7.0–8.9 Target fix: 30 days	CVSS 9.0–10.0 Target fix: 30 days*

** Critical vulnerabilities under active exploitation should be prioritised for the fastest possible remediation, even ahead of the 30-day target.*

Where a fix cannot be delivered within the target timeframe, Wavecom will notify

the reporter in advance with a revised date and, where available, interim mitigation guidance.

> *CRA / prEN 40000-1-3: [RMD-3-RQ-01]: The remediation must be tested before being released to confirm it resolves the vulnerability and does not introduce new issues.*

Before releasing any fix, we will verify that the remediation resolves the reported vulnerability and does not introduce new security weaknesses. For critical and high severity issues, testing will include functional verification and, where appropriate, regression testing.

6.4 Coordinated Public Disclosure

We support coordinated disclosure. This means we will collaborate with the vulnerability reporter to agree a date for publicly sharing information about the vulnerability, once a fix is available.

> *CRA Annex I Part II, point (4): Information about fixed vulnerabilities must be publicly disclosed, including description, affected versions, severity, and remediation guidance. prEN 40000-1-3: [PRE-2-RC-02]: The policy should include details about the publication procedure. [PRE-2-RC-03]: Disclosure must be coordinated to avoid premature publication.*

WAVECOM aims to complete coordinated disclosure within 90 calendar days of the acknowledgement date. Where this cannot be met, we will contact the reporter before the deadline to agree a revised date.

Important — Right to Disclose: Where it is necessary to protect users or to comply with applicable legal obligations, **WAVECOM** reserves the right to disclose vulnerability information publicly without the reporter's prior agreement or involvement.

Where both parties agree on an embargo period — a period during which neither side will publish information about the vulnerability — the agreed period and end date (disclosure date) will be documented in writing. Either party may request an extension to the embargo with reasonable justification.

Once a fix is released, Wavecom will:

- Notify the reporter that the vulnerability has been resolved.

- Publish a security advisory, release note, or product notification.
- Credit the reporter in any public advisory, with their consent.

7. Single Reporting Platform (SRP)

> *Further information: Regulation - 2024/2847 - EN - EUR-Lex. (65)*

Definitions

Actively Exploited Vulnerability: Security Incident where an active vulnerability on the product is exploited by a malicious actor.

Severe Incident: Security Incident where the security features of the product are impacted significantly, and where its category cannot be defined as an “Actively exploited Vulnerability”.

7.1 Information gathering mechanisms

Channel	Definition	Details
Customers enquiries	Customers are periodically asked about any security incidents involving the products.	Owner: Commercial Department and Technical Support. Security is included in the periodic customer service reviews and in field interventions. Records are kept in the incident tracker; any indication of exploitation is escalated immediately to the ISM.
Threat Intelligence	Monitor commercial or open-source exploitation reports	Advisories from CNCS and CERT.PT, ENISA publications, CVE feeds correlated with the component inventory (SBOM) of WaveOS and of the platforms (IoT Manager, CAS and WHERE IS), and bulletins from suppliers and ODM/OEM partners (RAK, Supermicro, Kontron, Quectel, SimCom and cloud providers).

Channel	Definition	Details
Vulnerability submission	Assess vulnerabilities received through the vulnerability reporting channels to determine whether they are actively exploited.	Reports received at ciberseguranca@wavecom.pt under the Wavecom Coordinated Vulnerability Disclosure Policy are triaged by the ISM, who determines whether there is reliable evidence of active exploitation.
Internal Vulnerability management	Assess internally identified vulnerabilities to determine if they are actively exploited	Findings from the secure development lifecycle (SGSI_PLT10), internal and third-party testing, and monitoring and log review of the SaaS platforms (IoT Manager, CAS, WHERE IS®) are assessed for evidence of active exploitation.
Other		Internal escalation: any employee, contractor or field engineer who receives an indication of active exploitation reports it immediately to the ISM, in writing, without prior technical assessment and without hierarchical filtering.

7.2 ENISA reports

The following reports will be sent to ENISA single reporting platform:

- https://portal.cra-srp.enisa.europa.eu/

Report Type	Deadline (from detection)	Report Content
Early warning	24h	Notification type (vulnerability / Incident) Notification level (24h,72h, Final) Name of manufacturer or steward Product Title

Report Type	Deadline (from detection)	Report Content
Vulnerability/ Incident Notification	72h	Early warning content Nature of the vulnerability Nature of the exploit Corrective or mitigating measures taken Corrective or mitigating measures that the users can take. Sensitivity of information (If applicable)
Final Report (Vulnerabilities)	14 days	Vulnerability / Incident notification content Date when corrective or mitigating measure has been available. Full description of the vulnerability Severity of the vulnerability Impact of the vulnerability Malicious actor that has exploited the vulnerability Details about the security update / corrective measures available.
Final Report (Severe Incidents)	1 month	Vulnerability / Incident notification content Detailed description of the incident Severity of the incident. Impact of the incident. Type of threat or root cause that has triggered the incident. Applied and ongoing mitigation measures.

8. Confidentiality and Anonymous Reporting

> *prEN 40000-1-3: [PRE-5-RC-03]: Reporters have the possibility to submit reports anonymously.*

We will treat all vulnerability reports with confidentiality. Personal information provided by reporters will not be shared with third parties without explicit consent, except where required by applicable law.

Reporters who wish to remain anonymous may submit reports through any of the channels listed above without providing personal details. Please note that anonymous reports may limit our ability to provide status updates or formal recognition.

Anonymous reports are accepted and are triaged on the same terms as attributed reports. Reporters should note that where no contact details are provided, we cannot request clarification, agree a coordinated disclosure date, or provide status updates.

9. Contact Information

Field	Details
Security Contact	ciberseguranca@wavecom.pt
Postal Address	WAVECOM – Soluções Rádio, S.A. Rua das Cardadeiras, 107 3800-125 Aveiro, Portugal
PGP Public Key	Available on request.
Response Hours	09:00–18:00 Europe/Lisbon, Monday to Friday, excluding Portuguese public holidays. Reports indicating active exploitation are escalated outside these hours through the permanent escalation contact.
Escalation Contact	Information Security Manager (ISM), as the CRA single point of contact. Escalation contacts are documented in SGSI_PLT19 (List of Authority Contacts).

10. Policy Management

10.1 Review and Update

This policy will be reviewed at least annually, or sooner following any significant change to the product range, the security team, or the regulatory environment. Updated versions will be published on Wavecom's website and communicated internally.

Field	Wavecom
Where will this policy be published?	https://www.wavecom.pt/security (to be confirmed), with a security.txt file at https://www.wavecom.pt/.well-known/security.txt and a reference in the product documentation.
Who is responsible for reviewing it?	Information Security Manager (ISM)
Next review date	September 2027, or earlier following a significant product change or a change in the applicable CRA framework

10.2 Exemptions

Any exceptions to this policy must be approved by the document owner and recorded in the exceptions register. All exceptions are time-limited and reviewed annually.

11. Document History

Version	Date	Author	Description of Change
1.0	8th September 2026	Information Security Manager (ISM)	Initial release, adapted from the Eurofins CVD policy template v1.0